Ihre POLIZEI
Votre POLICE
La vostra POLIZIA

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

SKPPSC

Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

FICHE TECHNIQUE *ARNAQUES AU FAUX SUPPORT TECHNIQUE (ARNAQUES MICROSOFT)*

Déroulement de l'escroquerie

Au téléphone, des criminels se font souvent passer pour des employés de Microsoft ou d'un centre d'assistance informatique. Le prétexte de leur appel peut être par exemple une infection par virus, un problème de lenteur du système ou tout autre problème d'ordre technique. Leur véritable intention consiste en revanche à convaincre leur interlocuteur de leur laisser prendre le contrôle à distance de l'appareil, de télécharger un programme ou encore de consulter un site piraté mais en apparence parfaitement identique au site officiel dans le seul but de voler les identifiants de l'utilisateur.

D'une manière ou d'une autre, les escrocs réussissent à accéder directement au dispositif de leurs victimes pour ensuite intercepter leurs mots de passe ou télécharger les informations stockées sur leur ordinateur, ceci afin de mieux prendre le contrôle de la vie numérique de l'utilisateur. Les prétendus services d'assistance étant parfois payants, ceux-ci peuvent aller jusqu'à demander à leurs victimes de communiquer leur numéro de carte de crédit qu'ils utiliseront ensuite de manière abusive.

Dans le clip vidéo de la deuxième partie de la campagne nationale de prévention du 8 septembre 2020, relatant l'histoire de la mésaventure de Simon qui a laissé Martin prendre frauduleusement le contrôle de son ordinateur, ce dernier utilise un tel mode opératoire.

Les personnes qui appellent parlent souvent un mauvais anglais. Néanmoins, comme les numéros d'appel sont susceptibles d'être manipulés, la victime peut ainsi reconnaître sur l'écran de son téléphone le véritable numéro de la société en question.

Il arrive aussi de plus en plus que ces soi-disant opérateurs de centre d'assistance se fassent appeler par leurs propres victimes. Le mode opératoire est alors le suivant : en surfant sur internet, une fenêtre de type publicitaire (pop-up) s'affiche à l'écran, informant l'internaute d'un prétendu problème technique. La fenêtre reporte un numéro de téléphone suisse à appeler pour résoudre le problème. C'est là que les escrocs entrent en jeu et parviennent à obtenir de l'argent de leur victime pour de prétendus programmes anti-virus.

Pourquoi tant de gens se font avoir ?

En fait, nombreux sont ceux qui perdent pied quand on leur dit que les données stockées sur leur ordinateur sont menacées. Comme les escrocs argumentent de façon très professionnelle et proposent dans la foulée une solution au problème (à savoir leur assistance en ligne), il n'est pas étonnant que beaucoup acceptent cette aide avec reconnaissance. De plus, il est

facile pour les malfrats d'usurper un numéro de téléphone existant, par exemple celui d'une helpline, pour endormir la méfiance de leur cible, qui voyant s'afficher un numéro suisse, pense que ce sont des membres d'une société informatique qui lui veulent du bien.

Quelques chiffres

Si la criminalité « classique » correspondant à des infractions contre le patrimoine comme les cambriolages a largement baissé en Suisse (- 50,6% entre 2012, année record, et 2019), les nouvelles technologies permettent avec grande vraisemblance l'essor et le développement de nouveaux modes opératoires caractéristiques d'une criminalité « numérique ». A l'heure actuelle, il n'existe pas de statistique officielle au niveau national pour les arnaques au faux support technique (arnaques Microsoft), mais sur les 286 207 infractions contre le patrimoine commises dans notre pays en 2019, 17 606 représentent des escroqueries, soit 6.2%. En comparaison avec l'année 2018, ces dernières ont augmenté de 7.9% et une partie de cette majoration est très probablement due au développement des modes opératoires numériques.

Conseils

A garder en tête :

Qu'il s'agisse de Microsoft ou d'une tout autre société informatique (services de support ou d'assistance), relevons qu'il est extrêmement rare que des sociétés informatiques appellent spontanément pour proposer des prestations sans y avoir été sollicitées. En cas de problème technique, la prise de contact doit toujours se faire sur l'initiative du client et auprès d'une société reconnue comme telle ou proche de son domicile.

Pour se protéger :

- Mettez fin à tous les appels non sollicités provenant de soi-disant opérateurs de Microsoft ou d'autres services d'assistance informatique.
- Ne vous fiez pas au numéro qui s'affiche sur l'écran de votre téléphone.
- Ne communiquez jamais vos données personnelles (mots de passe ou numéros de cartes de crédit) à d'autres personnes.
- Ne laissez personne prendre le contrôle à distance de votre ordinateur.
- Ne téléchargez jamais de logiciels gratuits à partir de sites internet non fiables.
- En cas de besoin, composez toujours les numéros de téléphone officiels de Microsoft ou des services d'assistance que vous trouverez sur le site officiel de ce géant.
- Pour contacter votre institut bancaire, utilisez exclusivement les numéros de téléphone officiels que vous retrouverez par exemple sur vos extraits de compte.

S'il est trop tard et que vous avez déjà permis à quelqu'un d'accéder à votre ordinateur :

- Coupez immédiatement la connexion internet et éteignez votre appareil.
- Ne rallumez votre appareil que lorsque le réseau est désactivé (par ex. wifi désactivé) et analysez immédiatement l'ensemble de votre disque dur avec un programme antivirus.
- Modifiez tous vos mots de passe.
- N'hésitez pas à demander l'aide d'un professionnel si vous n'êtes pas sûr de vous.

- Si vous avez communiqué des données confidentielles (par ex. des données bancaires ou des informations concernant votre carte de crédit), contactez immédiatement la société de cartes de crédit et/ou votre institut bancaire afin de faire bloquer les transactions en cours et votre compte.
- Vous pouvez ensuite contacter votre police locale.

Parole de victime[1]

« Alors que je ne connais pas très bien l'informatique et qu'il avait l'air de bien s'y connaitre, ben, je lui ai fait confiance et je lui ai dit, bon d'accord, et il m'a dit, ben, pour régler ce problème, il faut que je prenne le contrôle de l'ordinateur. Comme je sais que cela peut être dangereux quand même, j'ai un peu hésité mais au final j'ai laissé faire. »

[1] Témoignage de victime paru sur le journal télévisé 20 Heures de France 2 du 6 août 2014